



Lab-27: Configuring SIEM for GreenBloom Security Operations

Tatiana Meneses

February 17th, 2025

Overview

GreenBloom has been expanding its cybersecurity operations, and the executive team has prioritized improving threat detection capabilities. To achieve this, your team has been tasked with deploying and configuring a Security Information and Event Management (SIEM) solution using Elastic Stack. This will allow GreenBloom to centralize security logs, analyze threats in real time, and enhance its incident response capabilities.

Objectives

This lab will guide you through detecting and analyzing a simulated cyber attack using Elastic Security (SIEM). You will follow the Cyber Kill Chain attack phases, track malicious activity in Kibana, and create a detection and response report.

You will configure **Winlogbeat** to collect and analyze Windows event logs using an existing Elastic. You will install and configure Winlogbeat on a Windows 10 machine to monitor failed login attempts.

This exercise will help you understand how to integrate Windows event logs into an Elastic-based SIEM solution for security monitoring.

Your objective in this lab is to:

1. **Set up and configure Elastic SIEM** to collect and analyze security logs from GreenBloom's environment.
2. **Validate SIEM functionality** by executing **Atomic Red Team tests**—simulated attack techniques designed to test detection effectiveness.

Requirements

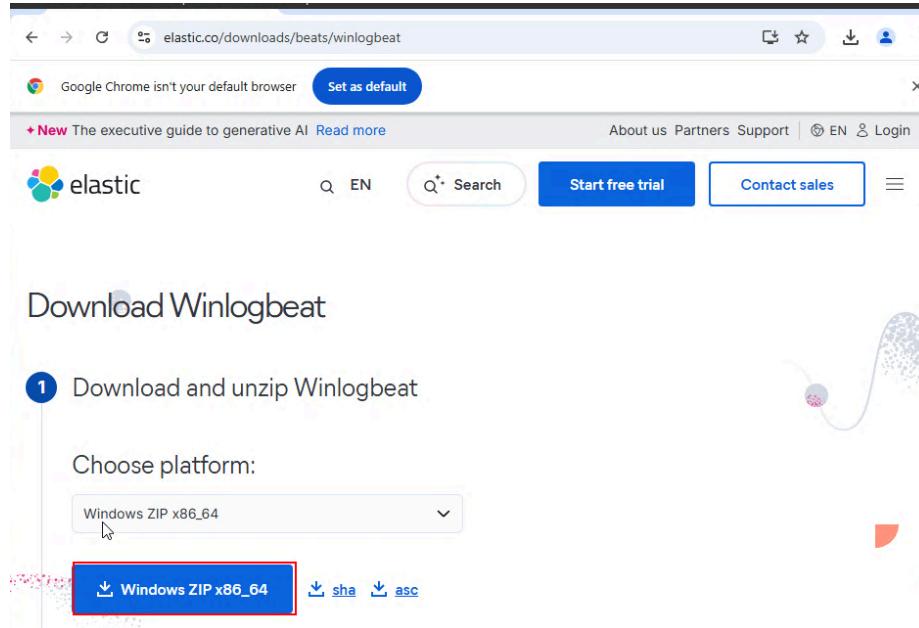
A virtualized environment with Ubuntu and Windows 10 VMs

Pre-installed and running Elastic

Network configuration set to NAT Network or Bridge Adapter

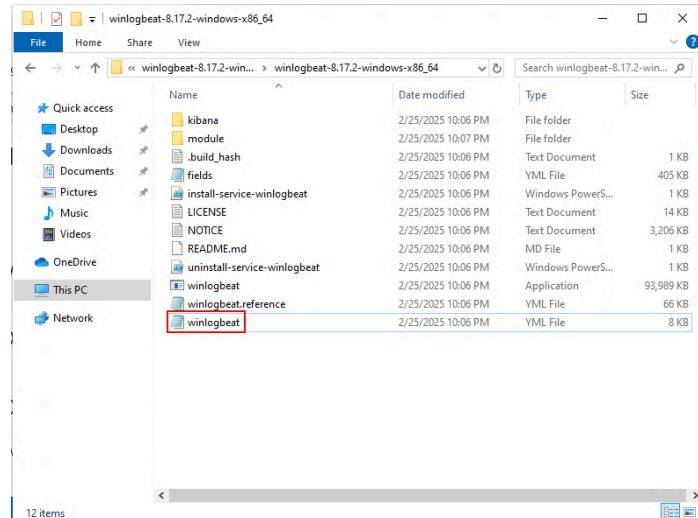
Part 1: Configure Winlogbeat

Download Winlogbeat: <https://www.elastic.co/downloads/beats/winlogbeat>



The screenshot shows the Elastic website's download page for Winlogbeat. At the top, there's a navigation bar with links for 'About us', 'Partners', 'Support', 'EN', 'Login', and buttons for 'Start free trial' and 'Contact sales'. Below the navigation, there's a search bar and a 'Set as default' button for Google Chrome. A banner at the top says '+ New The executive guide to generative AI' with a 'Read more' link. The main content area has a heading 'Download Winlogbeat' and a step-by-step guide. Step 1, 'Download and unzip Winlogbeat', is shown with a sub-instruction 'Choose platform:' and a dropdown menu set to 'Windows ZIP x86_64'. Below the dropdown are download links: 'Windows ZIP x86_64' (highlighted with a red box), 'sha', and 'asc'.

Edit `winlogbeat.yml` before installation:



- Change "Array of hosts" to your Elastic IP.
- Comment the API key line and uncomment username/password, filling in the correct credentials.

```

File Edit Format View Help
# ===== Outputs =====
# Configure what output to use when sending the data collected by the beat.

# ----- Elasticsearch Output -----
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["192.168.1.103:9200"]

  # Protocol - either `http` (default) or `https`.
  #protocol: "https"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  username: "elastic"
  password: "████████"

  # Pipeline to route events to security, sysmon, or powershell pipelines.
  pipeline: "winlogbeat-%{[agent.version]}-routing"
]

# ----- Logstash Output -----
#output.logstash:
  # The Logstash hosts
<   >

```

Ln 114, Col 25 | 100% | Unix (LF) | UTF-8

- Update Kibana hosts to your Elastic IP.

```

File Edit Format View Help
#setup.dashboards.url:

# ===== Kibana =====
# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:

  # Kibana Host
  # Scheme and port can be left out and will be set to the default (http and 5601)
  # In case you specify an additional path, the scheme is required: http://localhost:5601/
  # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
  host: "192.168.1.103:5601"

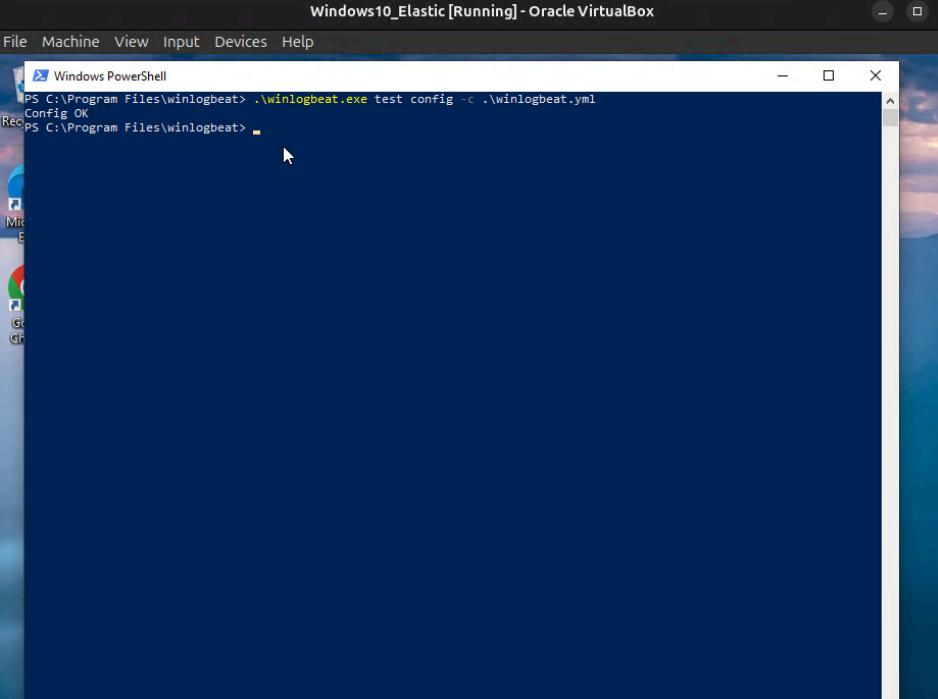
  # Kibana Space ID
  # ID of the Kibana Space into which the dashboards should be loaded. By default,
  # the Default Space will be used.
  #space.id:

# ===== Elastic Cloud =====
# These settings simplify using Winlogbeat with the Elastic Cloud (https://cloud.elastic.co)
# The cloud.id setting overwrites the `output.elasticsearch.hosts` and
<   >

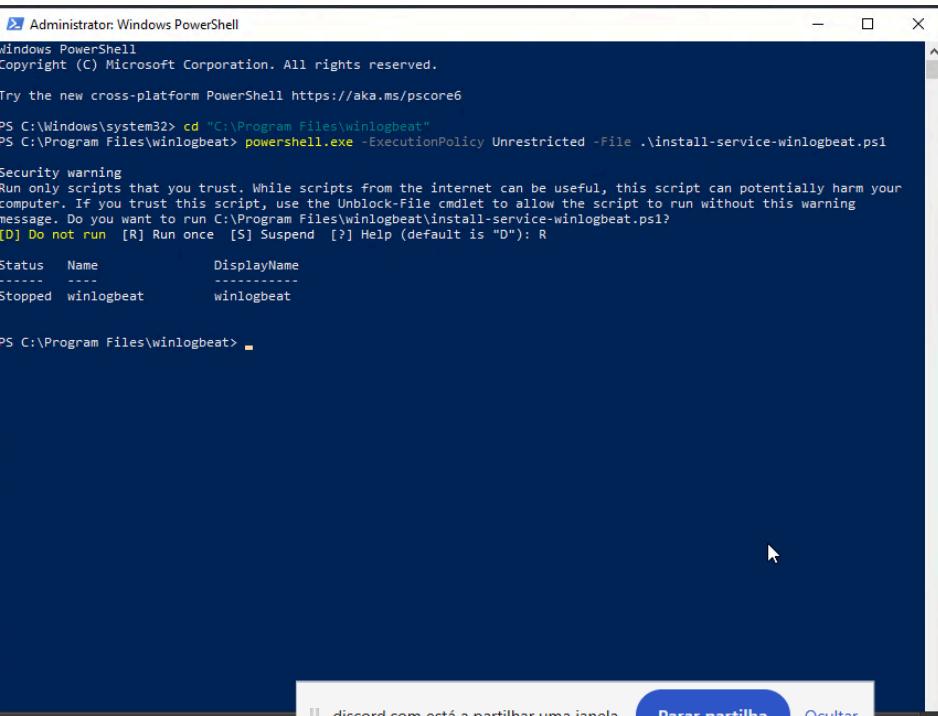
```

Ln 88, Col 1 | 100% | Unix (LF) | UTF-8

- Install Winlogbeat on the Windows 10 machine.



```
Windows10_Elastic [Running] - Oracle VirtualBox
File Machine View Input Devices Help
PS C:\Program Files\winlogbeat> .\winlogbeat.exe test config -c .\winlogbeat.yml
Config OK
PS C:\Program Files\winlogbeat>
```

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

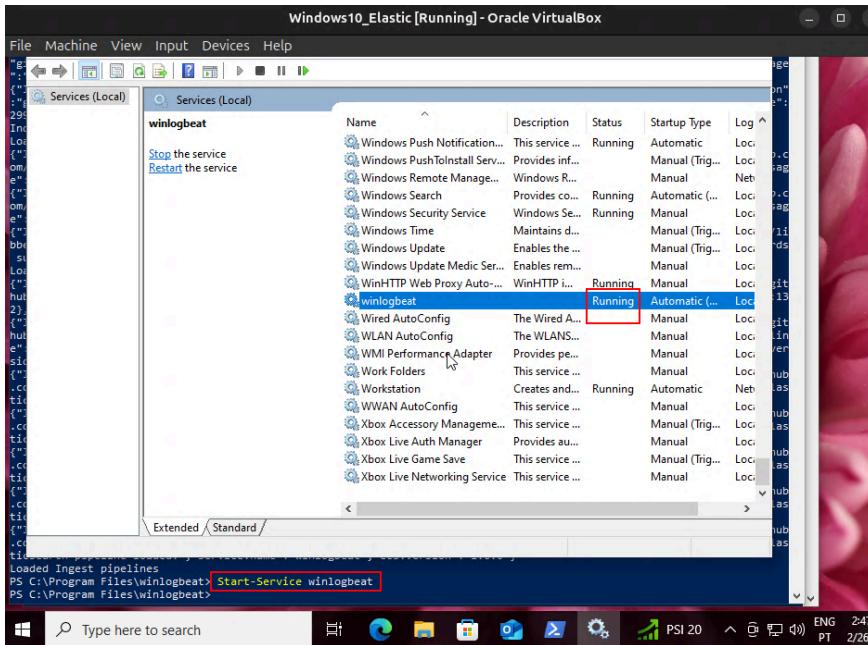
PS C:\Windows\system32> cd "C:\Program Files\winlogbeat"
PS C:\Program Files\winlogbeat> powershell.exe -ExecutionPolicy Unrestricted -File .\install-service-winlogbeat.ps1

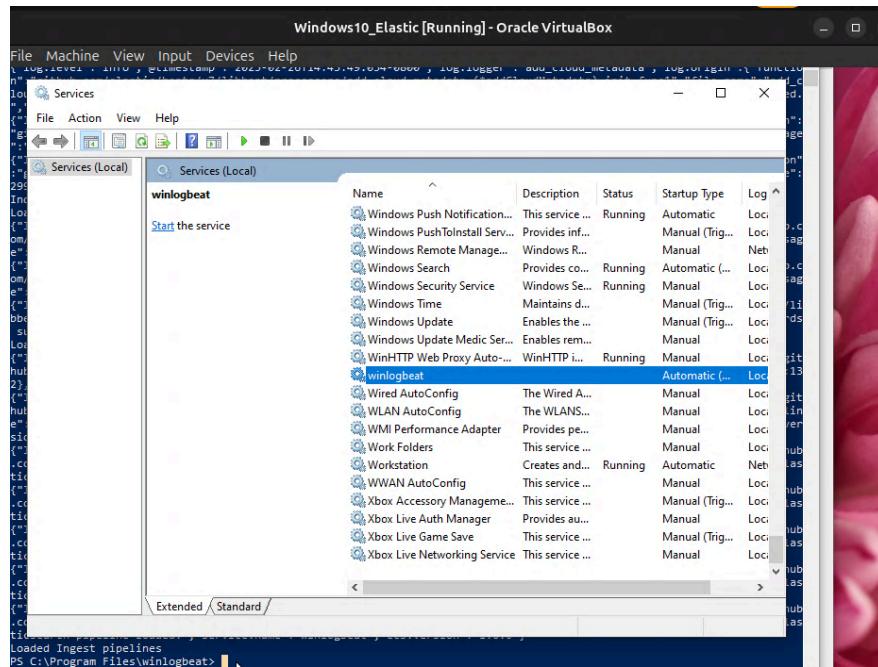
Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your
computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning
message. Do you want to run C:\Program Files\winlogbeat\install-service-winlogbeat.ps1?
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"): R

Status   Name           DisplayName
-----  --  -----
Stopped  winlogbeat    winlogbeat

PS C:\Program Files\winlogbeat>
```

```
Windows10_Elastic [Running] - Oracle VirtualBox
File Machine View Input Devices Help
load_metadata.go:100, message: "load_metadata: hosting provider type not detected", "service.name": "winlogbeat", "ecs.version": "1.6.0"
("log.level": "info", "@timestamp": "2025-02-26T14:43:51.113-0800", "log.logger": "template_loader", "log.origin": {"function": "github.com/elastic/beats/v7/libbeat/template.(*ESLoader).Load", "file.name": "template/load.go", "file.line": 168}, "message": "Data stream with name \"winlogbeat-8.17.1\" loaded.", "service.name": "winlogbeat", "ecs.version": "1.6.0"}
("log.level": "info", "@timestamp": "2025-02-26T14:43:51.127-0800", "log.logger": "index-management", "log.origin": {"function": "github.com/elastic/beats/v7/libbeat/indexManagement.(IndexManager).Setup", "file.name": "idxmgmt/index_support.go", "file.line": 299}, "message": "Loaded index template.", "service.name": "winlogbeat", "ecs.version": "1.6.0"}
Index setup finished.
Loading dashboards (Kibana must be running and reachable)
("log.level": "info", "@timestamp": "2025-02-26T14:43:51.132-0800", "log.logger": "kibana", "log.origin": {"function": "github.com/elastic/elastic-agent-lbs/kibana.NewClientWithConfigDefault", "file.name": "kibana/client.go", "file.line": 181}, "message": "Kibana url: http://192.168.1.106:5601", "service.name": "winlogbeat", "ecs.version": "1.6.0"}
("log.level": "info", "@timestamp": "2025-02-26T14:43:51.629-0800", "log.logger": "kibana", "log.origin": {"function": "github.com/elastic/elastic-agent-lbs/kibana.NewClientWithConfigDefault", "file.name": "kibana/client.go", "file.line": 181}, "message": "Kibana url: http://192.168.1.106:5601", "service.name": "winlogbeat", "ecs.version": "1.6.0"}
("log.level": "info", "@timestamp": "2025-02-26T14:44:03.098-0800", "log.origin": {"function": "github.com/elastic/beats/v7/libbeat/cmd/instance.(*Beat).loadDashboards", "file.name": "instance/beat.go", "file.line": 1306}, "message": "Kibana dashboards successfully loaded.", "service.name": "winlogbeat", "ecs.version": "1.6.0"}
Loaded dashboards
("log.level": "info", "@timestamp": "2025-02-26T14:44:03.107-0800", "log.logger": "esclientleg", "log.origin": {"function": "github.com/elastic/beats/v7/libbeat/esleg.NewConnection", "file.name": "eslegclient/connection.go", "file.line": 132}, "message": "elasticsearch search url: http://192.168.1.106:9200", "service.name": "winlogbeat", "ecs.version": "1.6.0"}
("log.level": "info", "@timestamp": "2025-02-26T14:44:03.138-0800", "log.logger": "esclientleg", "log.origin": {"function": "github.com/elastic/beats/v7/libbeat/esleg.NewConnection", "file.name": "eslegclient/connection.go", "file.line": 323}, "message": "Attempting to connect to Elasticsearch version 8.17.2 (default)", "service.name": "winlogbeat", "ecs.version": "1.6.0"}
("log.level": "info", "@timestamp": "2025-02-26T14:44:04.017-0800", "log.logger": "pipeline", "log.origin": {"function": "github.com/elastic/beats/v7/filebeat/fileset.LoadPipeline", "file.name": "fileset/pipelines.go", "file.line": 135}, "message": "Elasticsearch pipeline loaded.", "service.name": "winlogbeat", "ecs.version": "1.6.0"}
("log.level": "info", "@timestamp": "2025-02-26T14:44:04.544-0800", "log.logger": "pipeline", "log.origin": {"function": "github.com/elastic/beats/v7/filebeat/fileset.LoadPipeline", "file.name": "fileset/pipelines.go", "file.line": 135}, "message": "Elasticsearch pipeline loaded.", "service.name": "winlogbeat", "ecs.version": "1.6.0"}
("log.level": "info", "@timestamp": "2025-02-26T14:44:04.928-0800", "log.logger": "pipeline", "log.origin": {"function": "github.com/elastic/beats/v7/filebeat/fileset.LoadPipeline", "file.name": "fileset/pipelines.go", "file.line": 135}, "message": "Elasticsearch pipeline loaded.", "service.name": "winlogbeat", "ecs.version": "1.6.0"}
("log.level": "info", "@timestamp": "2025-02-26T14:44:06.000-0800", "log.logger": "pipeline", "log.origin": {"function": "github.com/elastic/beats/v7/filebeat/fileset.LoadPipeline", "file.name": "fileset/pipelines.go", "file.line": 135}, "message": "Elasticsearch pipeline loaded.", "service.name": "winlogbeat", "ecs.version": "1.6.0"}
("log.level": "info", "@timestamp": "2025-02-26T14:44:06.516-0800", "log.logger": "pipeline", "log.origin": {"function": "github.com/elastic/beats/v7/filebeat/fileset.LoadPipeline", "file.name": "fileset/pipelines.go", "file.line": 135}, "message": "Elasticsearch pipeline loaded.", "service.name": "winlogbeat", "ecs.version": "1.6.0"}
Loaded Ingest pipelines
PS C:\Program Files\winlogbeat>
```





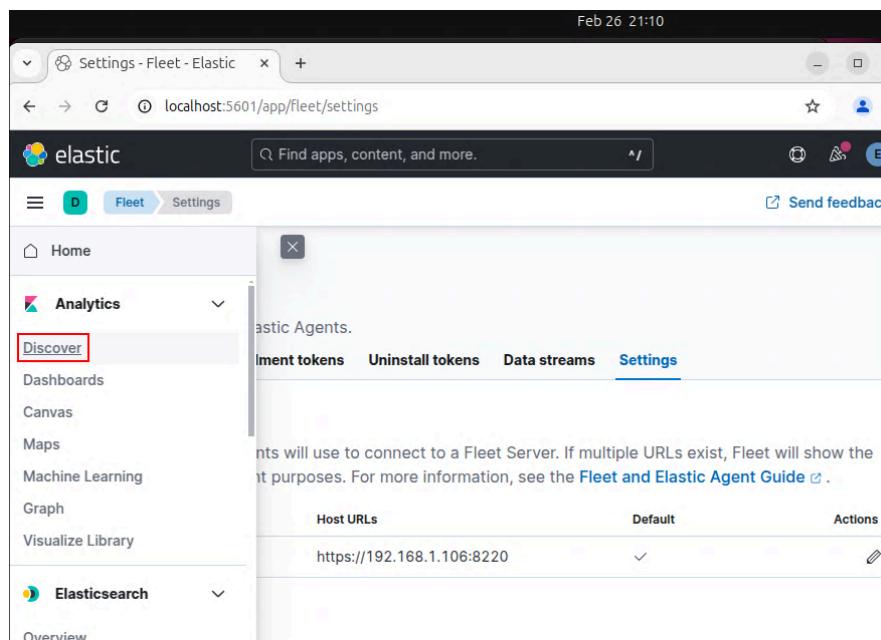
Part 2: Generate and Analyze Event Logs

1. Generate system activity

Perform several failed login attempts on the Windows 10 machine.

On Elastic, navigate to:

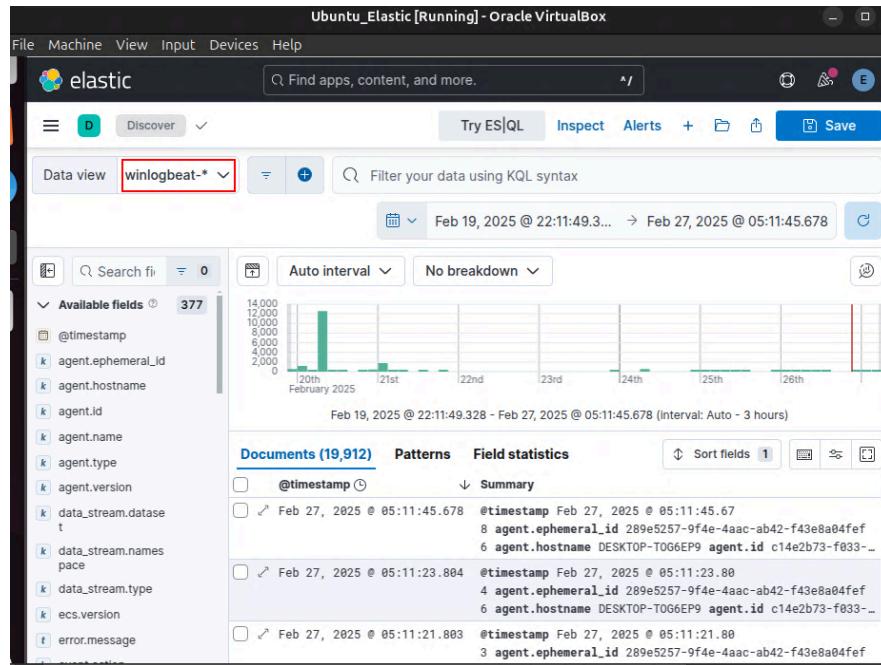
Analytics > Discover



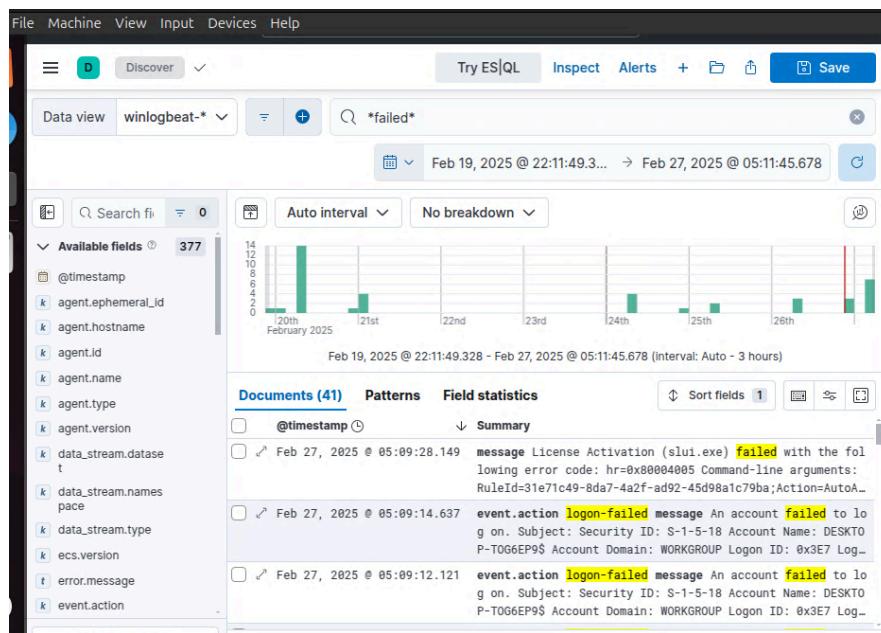
The screenshot shows the Elasticsearch Analytics Discover interface. The left sidebar has a red box around the 'Discover' tab under the 'Analytics' section. The main area displays a table with columns: Host URLs, Default, and Actions. There is one row with the URL 'https://192.168.1.106:8220'. The top right corner shows the date 'Feb 26 21:10'.

| Host URLs | Default | Actions |
|----------------------------|---------|---------|
| https://192.168.1.106:8220 | ✓ | edit |

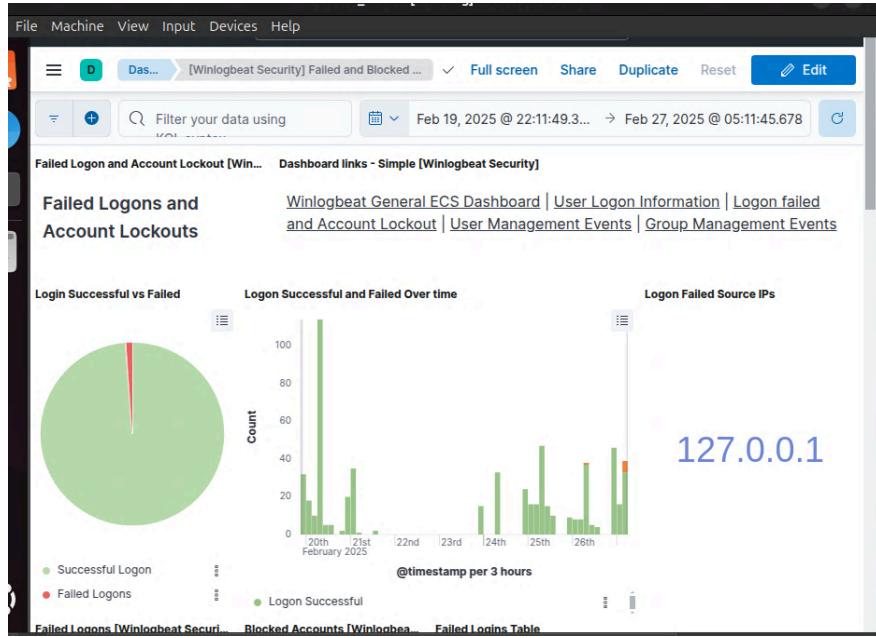
- Change Data Views to winlogbeat



- Check for failed login attempts.



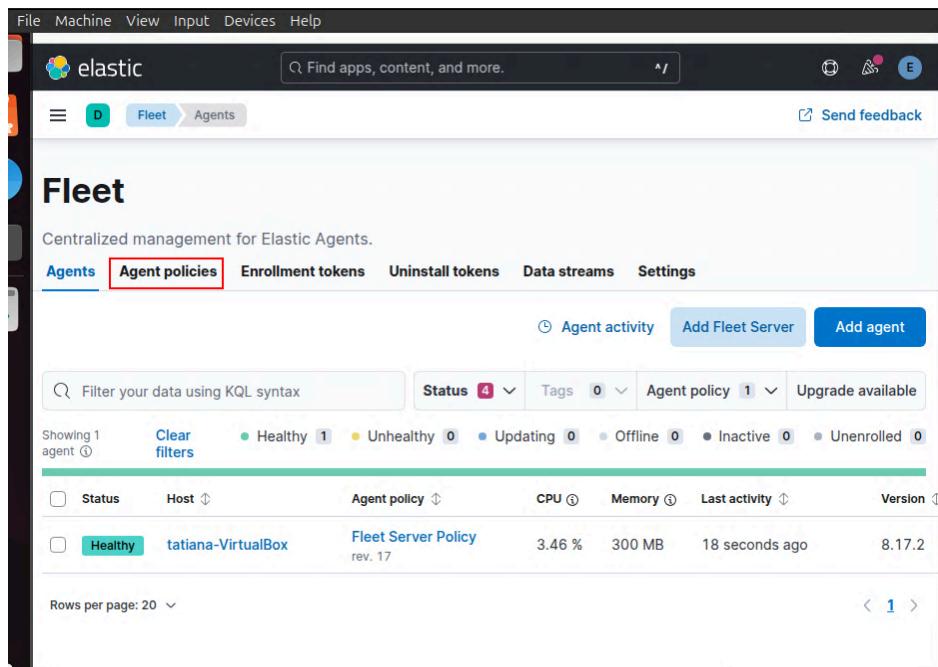
- If needed, refer to the [official Winlogbeat documentation](#) for event IDs
- For a more visual representation, check dashboards at: **Analytics -> Dashboard**



2. Install an agent on the Windows 10 machine

Go to "Agent policies" and create a new policy with 'System' and 'Elastic Defend'.

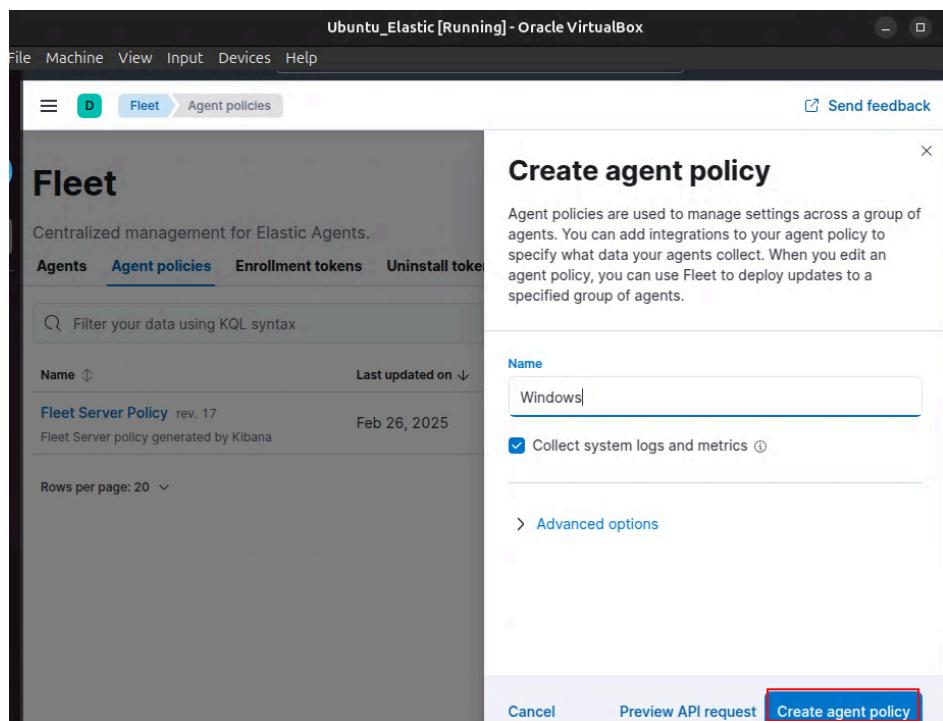
1. To add a new agent policy, we go to Fleet;



The screenshot shows the Fleet interface with the 'Agent policies' tab selected. A single healthy agent, 'tatiana-VirtualBox', is listed under the 'Fleet Server Policy'. The interface includes a search bar, status filters, and a table view.

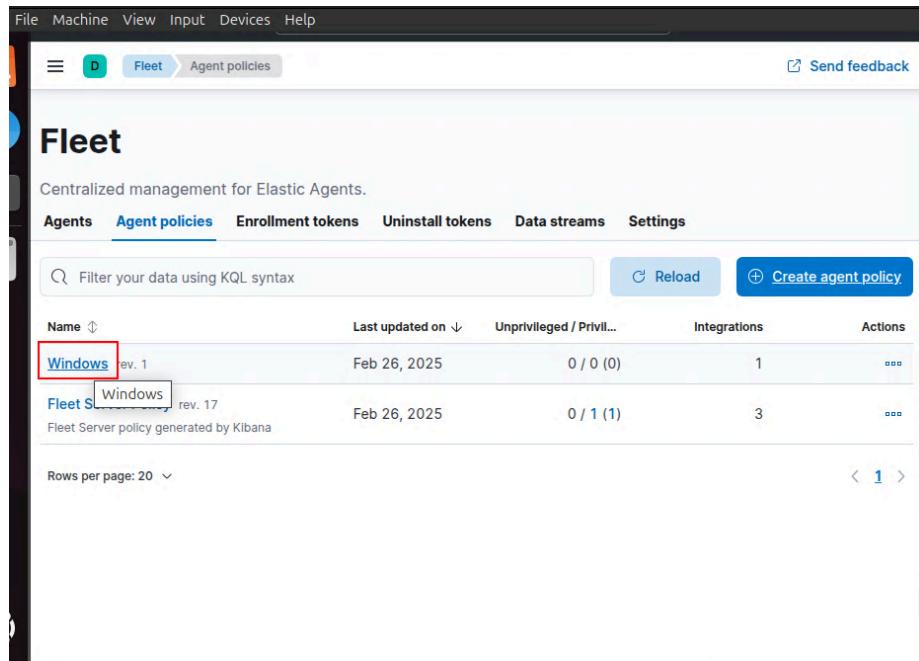
| Status | Host | Agent policy | CPU | Memory | Last activity | Version |
|---------|--------------------|--------------------------------|--------|--------|----------------|---------|
| Healthy | tatiana-VirtualBox | Fleet Server Policy rev. 17 | 3.46 % | 300 MB | 18 seconds ago | 8.17.2 |

2. Select Agent Policies;



The screenshot shows the Fleet interface with the 'Agent policies' tab selected. A new agent policy is being created, named 'Windows'. The 'Collect system logs and metrics' checkbox is checked. The 'Create agent policy' button is highlighted with a red box.

3. Give a name to the new policy and then create it;



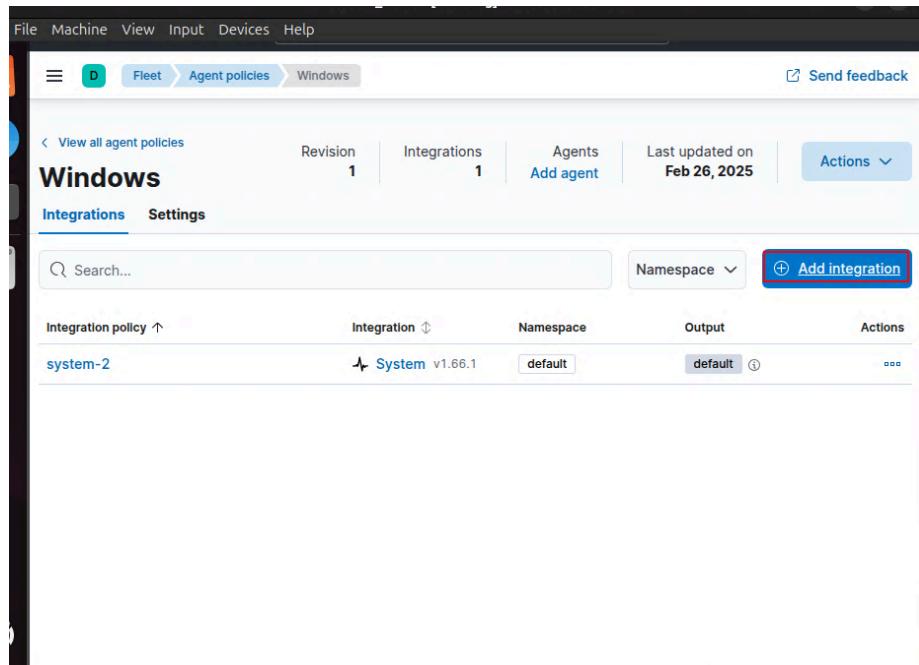
The screenshot shows the Fleet interface with the 'Agent policies' tab selected. A table lists two policies:

| Name | Last updated on | Unprivileged / Privil... | Integrations | Actions |
|-----------------------------------------|-----------------|--------------------------|--------------|---------|
| Windows rev. 1 | Feb 26, 2025 | 0 / 0 (0) | 1 | ... |
| Fleet S windows rev. 17 | Feb 26, 2025 | 0 / 1 (1) | 3 | ... |

Fleet Server policy generated by Kibana

Rows per page: 20 < 1 >

4. In order to add the integrations, we open the newly created policy;



The screenshot shows the 'Windows' agent policy details page. The 'Integrations' tab is selected. The page displays the following information:

- Revision: 1
- Integrations: 1
- Agents: Add agent
- Last updated on: Feb 26, 2025
- Actions: Actions ▾

Search bar: Search...

Add integration button: + Add integration

| Integration policy | Integration | Namespace | Output | Actions |
|--------------------|----------------|-----------|---------|---------|
| system-2 | System v1.66.1 | default | default | ... |

5. Select Add Integration

Integrations

Choose an integration to start collecting and analyzing your data.

[Browse integrations](#) [Installed integrations](#)

All categories **410**

- APM **1**
- AWS **42**
- Azure **29**
- Cloud **92**
- Containers **16**
- Custom **54**
- Database **39**
- Elastic Stack **51**

Search for integrations

APM
Collect performance metrics from your applications with Elastic APM.

Elastic Defend
Protect your hosts and cloud workloads with threat prevention, detection, and deep security data visibility.

Web crawler
Add search to your website with the web crawler.

Add Elastic Defend integration

Configure an integration for the selected agent policy.

Requires root privileges
Elastic Agent needs to be run with root/administrator privileges for this integration.

This package has 2 transform assets which will be created and started with the same roles as the user installing the package.

1 Configure integration

Integration settings
Choose a name and description to help identify how this integration will be used.

Integration name: Elastic Defend Integration
Description: Optional

[Advanced options](#)

[Cancel](#) [Save and continue](#)

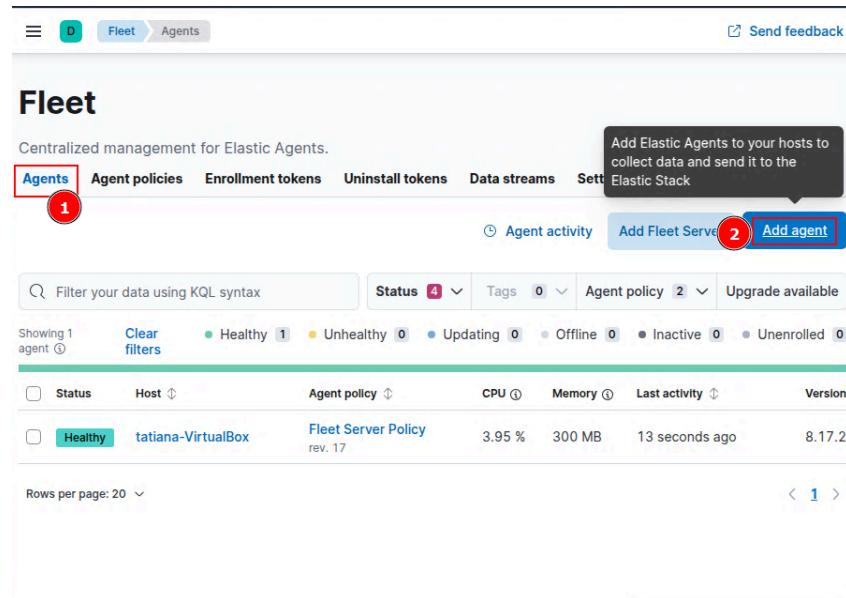
Fleet **Agent policies** **Windows** [Send feedback](#)

[View all agent policies](#) **Windows** **Revision 4** **Integrations 2** [Agents](#) [Add agent](#) **Last updated on Feb 26, 2025** [Actions](#)

Integrations [Settings](#)

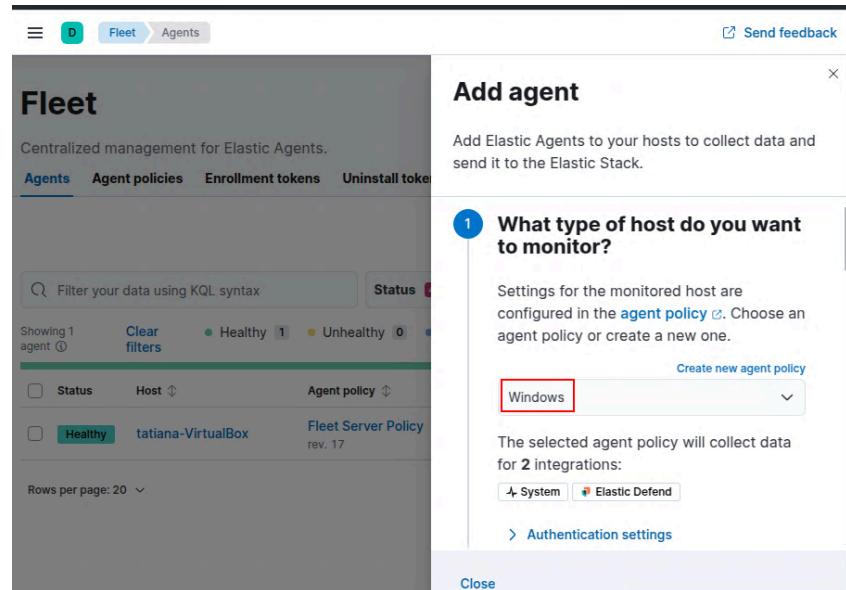
| Integration policy ↑ | Integration ↓ | Namespace | Output | Actions |
|----------------------------|------------------------------------------------------------------------------------------------------------|-----------|---------|---------|
| Elastic Defend Integration |  Elastic Defend v8.17.0 | default | default | ... |
| system-2 |  System v1.66.1 | default | default | ... |

6. Then select both integrations: System and Elastic Defend;



The screenshot shows the Fleet interface with the 'Agents' tab selected. At the top right, there is a tooltip: "Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack". Below the tabs, there are buttons for 'Agent activity', 'Add Fleet Server', and 'Add agent' (which is highlighted with a red circle labeled '2'). The main table shows one healthy agent named 'tatiana-VirtualBox' under the 'Fleet Server Policy'. The 'Add agent' dialog is partially visible on the right.

7. After adding the integrations, we need to add the agents;



The screenshot shows the 'Add agent' dialog box. It asks 'What type of host do you want to monitor?' and provides a dropdown menu with 'Windows' selected (highlighted with a red box). Below the dropdown, it says 'The selected agent policy will collect data for 2 integrations:' followed by 'System' and 'Elastic Defend' (both highlighted with red boxes). The 'Close' button is at the bottom.

Go Fleet -> Add Agent -> Choose the newly created policy.

On the powershell script to enroll a new machine, add an "--insecure" at the end of the command.

- The following command was run in PowerShell:

Add agent

Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.

- [Guide](#)
- System
- Elastic Defend

To install Elastic Agent without root privileges, add the `--unprivileged` flag to the `elastic-agent install` command below. For more information, see the [Fleet and Elastic Agent Guide](#).

Linux Tar Mac **Windows** RPM DEB Kubernetes

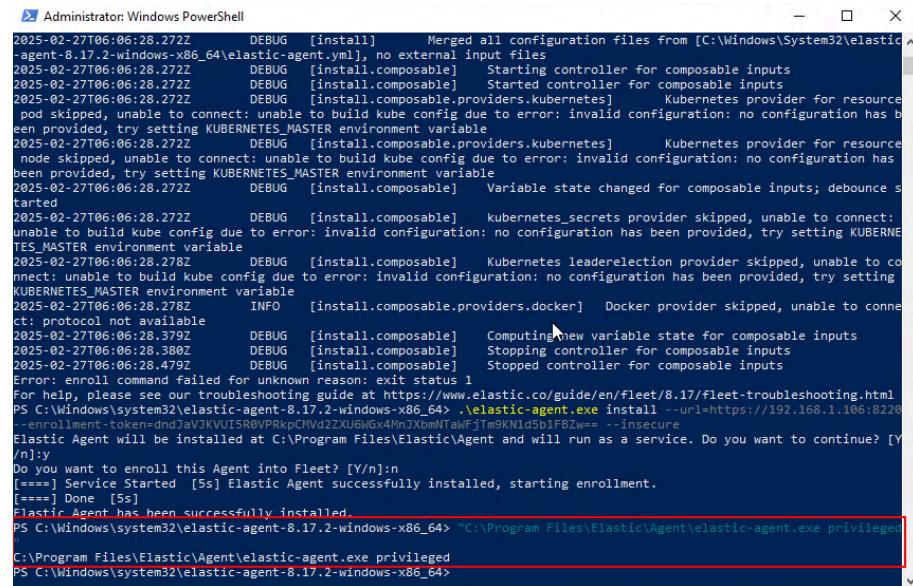
```
$ProgressPreference = 'SilentlyContinue'
Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent-8.17.2-windows-x86_64.zip -DestinationPath
Expand-Archive .\elastic-agent-8.17.2-windows-x86_64
cd elastic-agent-8.17.2-windows-x86_64
.\elastic-agent.exe install --url=https://192.168.1.106:8220 --enrollment-
```

Administrator: Windows PowerShell

```
12-windows-x86_64\elastic-agent.yaml
2025-02-27T06:06:28.272Z DEBUG [install] Merged configuration from C:\Windows\System32\elastic-agent-8.17
12-windows-x86_64\elastic-agent.yaml into result
2025-02-27T06:06:28.272Z DEBUG [install] Merged all configuration files from [C:\Windows\System32\elastic
-agent-8.17.2-windows-x86_64\elastic-agent.yaml], no external input files
2025-02-27T06:06:28.272Z DEBUG [install.composable] Starting controller for composable inputs
2025-02-27T06:06:28.272Z DEBUG [install.composable] Started controller for composable inputs
2025-02-27T06:06:28.272Z DEBUG [install.composable.providers.kubernetes] Kubernetes provider for resource
pod skipped, unable to connect: unable to build kube config due to error: invalid configuration: no configuration has b
een provided, try setting KUBERNETES_MASTER environment variable
2025-02-27T06:06:28.272Z DEBUG [install.composable.providers.kubernetes] Kubernetes provider for resource
node skipped, unable to connect: unable to build kube config due to error: invalid configuration: no configuration has
been provided, try setting KUBERNETES_MASTER environment variable
2025-02-27T06:06:28.272Z DEBUG [install.composable] Variable state changed for composable inputs; debounce s
tarted
2025-02-27T06:06:28.272Z DEBUG [install.composable] kubernetes_secrets provider skipped, unable to connect:
unable to build kube config due to error: invalid configuration: no configuration has been provided, try setting KUBERNE
TES_MASTER environment variable
2025-02-27T06:06:28.278Z DEBUG [install.composable] Kubernetes leaderelection provider skipped, unable to co
nnect: unable to build kube config due to error: invalid configuration: no configuration has been provided, try setting
KUBERNETES_MASTER environment variable
2025-02-27T06:06:28.278Z INFO [install.composable.providers.docker] Docker provider skipped, unable to conne
ct: protocol not available
2025-02-27T06:06:28.379Z DEBUG [install.composable] Computing new variable state for composable inputs
2025-02-27T06:06:28.380Z DEBUG [install.composable] Stopping controller for composable inputs
2025-02-27T06:06:28.479Z DEBUG [install.composable] Stopped controller for composable inputs
Error: enroll command failed for unknown reason: exit status 1
For help, please see our troubleshooting guide at https://www.elastic.co/guide/en/fleet/8.17/fleet-troubleshooting.html
PS C:\Windows\system32\elastic-agent-8.17.2-windows-x86_64>.\elastic-agent.exe install --url=https://192.168.1.106:8220
--enrollment-token=dndj3aJ3KVU15R8VPRpCMWdZZXU6WGX4lnJXdmNTaiFJTM9KNld5b1FBZw== --insecure
Elastic Agent will be installed at C:\Program Files\Elastic\Agent and will run as a service. Do you want to continue? [Y/n]:y
Do you want to enroll this Agent into Fleet? [Y/n]:n
[====] Service Started [5s] Elastic Agent successfully installed, starting enrollment.
[====] Done [5s]
Elastic Agent has been successfully installed.
PS C:\Windows\system32\elastic-agent-8.17.2-windows-x86_64>
```

Make sure the agent is running with privileges:

"C:\Program Files\Elastic\Agent\elastic-agent.exe privileged".



```

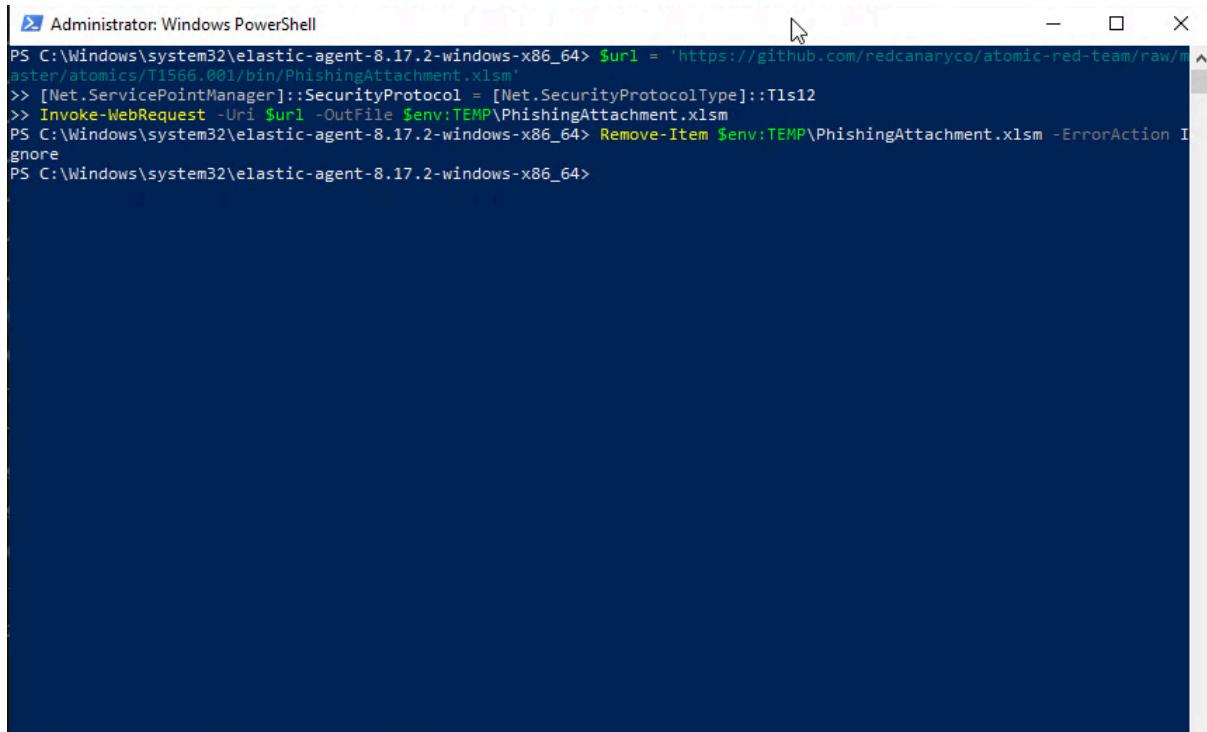
Administrator: Windows PowerShell
2025-02-27T06:06:28.272Z      DEBUG  [install]      Merged all configuration files from [C:\Windows\System32\elastic-agent-8.17.2-windows-x86_64\elastic-agent.yml], no external input files
2025-02-27T06:06:28.272Z      DEBUG  [install.composable]  Starting controller for composable inputs
2025-02-27T06:06:28.272Z      DEBUG  [install.composable]  Started controller for composable inputs
2025-02-27T06:06:28.272Z      DEBUG  [install.composable.providers.kubernetes]  Kubernetes provider for resource pod skipped, unable to connect: unable to build kube config due to error: invalid configuration: no configuration has been provided, try setting KUBERNETES_MASTER environment variable
2025-02-27T06:06:28.272Z      DEBUG  [install.composable.providers.kubernetes]  Kubernetes provider for resource node skipped, unable to connect: unable to build kube config due to error: invalid configuration: no configuration has been provided, try setting KUBERNETES_MASTER environment variable
2025-02-27T06:06:28.272Z      DEBUG  [install.composable]  Variable state changed for composable inputs; debounce started
2025-02-27T06:06:28.272Z      DEBUG  [install.composable]  kubernetes_secrets provider skipped, unable to connect: unable to build kube config due to error: invalid configuration: no configuration has been provided, try setting KUBERNETES_MASTER environment variable
2025-02-27T06:06:28.278Z      DEBUG  [install.composable]  Kubernetes leadership provider skipped, unable to connect: unable to build kube config due to error: invalid configuration: no configuration has been provided, try setting KUBERNETES_MASTER environment variable
2025-02-27T06:06:28.278Z      INFO   [install.composable.providers.docker]  Docker provider skipped, unable to connect: protocol not available
2025-02-27T06:06:28.379Z      DEBUG  [install.composable]  Computing new variable state for composable inputs
2025-02-27T06:06:28.380Z      DEBUG  [install.composable]  Stopping controller for composable inputs
2025-02-27T06:06:28.479Z      DEBUG  [install.composable]  Stopped controller for composable inputs
Error: enroll command failed for unknown reason: exit status 1
For help, please see our troubleshooting guide at https://www.elastic.co/guide/en/fleet/8.17/fleet-troubleshooting.html
PS C:\Windows\system32\elastic-agent-8.17.2-windows-x86_64> .\elastic-agent.exe install --url=https://192.168.1.106:8220
--enrollment-token=dndJaVjKVU15R0VPRkpCWd2ZXU6WGX4MnJXbmNTawFjtM9KN1dSb1FBZw== --insecure
Elastic Agent will be installed at C:\Program Files\Elastic\Agent and will run as a service. Do you want to continue? [Y/n]:
Do you want to enroll this Agent into Fleet? [Y/n]:n
[====] Service Started [5s] Elastic Agent successfully installed, starting enrollment.
[====] Done [5s]
Elastic Agent has been successfully installed.
PS C:\Windows\system32\elastic-agent-8.17.2-windows-x86_64> "C:\Program Files\Elastic\Agent\elastic-agent.exe privileged"
C:\Program Files\Elastic\Agent\elastic-agent.exe privileged
PS C:\Windows\system32\elastic-agent-8.17.2-windows-x86_64>

```

3. Run tests

Run this atomic test:

<https://www.atomicredteam.io/atomic-red-team/atomics/T1566.001#atomic-test-1---download-macro-enabled-phishing-attachment>



```

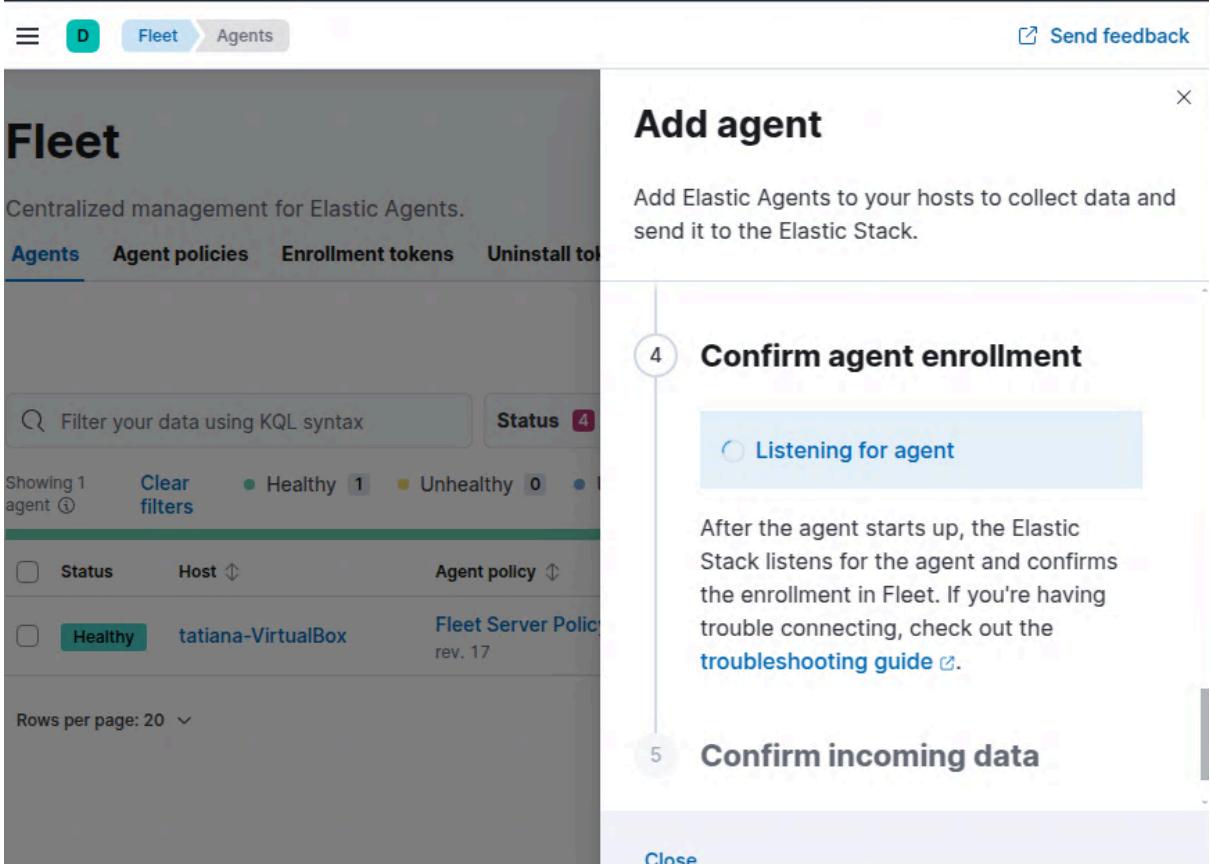
Administrator: Windows PowerShell
PS C:\Windows\system32\elastic-agent-8.17.2-windows-x86_64> $url = 'https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1566.001/bin/PhishingAttachment.xlsx'
>> [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
>> Invoke-WebRequest -Uri $url -OutFile $env:TEMP\PhishingAttachment.xlsx
PS C:\Windows\system32\elastic-agent-8.17.2-windows-x86_64> Remove-Item $env:TEMP\PhishingAttachment.xlsx -ErrorAction Ignore
PS C:\Windows\system32\elastic-agent-8.17.2-windows-x86_64>

```

4. Detect activities:

Go to "Observability" -> "Logs" and use file.name filter, to identify, creation of the

file, and the file deletion



The screenshot shows the Fleet interface with a modal overlay titled "Add agent". The modal contains instructions to "Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack." It shows a step 4: "Confirm agent enrollment" with a sub-step "Listening for agent". Below this, there is troubleshooting information: "After the agent starts up, the Elastic Stack listens for the agent and confirms the enrollment in Fleet. If you're having trouble connecting, check out the [troubleshooting guide](#)". Step 5: "Confirm incoming data" is also visible. On the left, the main Fleet interface shows a table of agents, with one entry for "tatiana-VirtualBox" listed as "Healthy".

Troubleshooting:

After all of the configurations were done in windows powershell, as shown in the previous printscreens, the agent does not start up.

Part 3: Documentation

To ensure GreenBloom maintains a strong security posture, your team must submit a detailed, step-by-step report documenting your entire configuration process. This documentation serves two key purposes:

Future Reference: Your team, and future analysts, will be able to replicate and refine this SIEM setup as GreenBloom's security needs evolve. A well-documented process ensures consistency in deployment and troubleshooting.

Company Records: As part of GreenBloom's cybersecurity services, detailed logs of

security implementations and testing procedures are essential for audits, compliance, and incident response planning.

Your report should include:

Setup Steps: A clear breakdown of how you configured Elastic SIEM, Winlogbeat, and other relevant components.

Testing Methodology: Details on how you executed Atomic Red Team tests, including the specific techniques used.

Detection and Analysis: Screenshots and explanations of security events detected in Kibana. **Challenges & Resolutions:** Any obstacles encountered and how you resolved them.

This documentation will be reviewed as part of your assessment and should be structured professionally, as if submitting it to GreenBloom's cybersecurity leadership.

By the end of this lab, you will have hands-on experience in SIEM deployment and testing, along with a valuable reference for future security operations. Now, let's secure GreenBloom!